Monitoring & Alerting Checklist

Security Best Practices for Small Teams

Low-overhead, high-impact security tips for lean IT teams and startups.

1. Access Control

- Use RBAC and least privilege
- Centralised identity (Azure AD, Okta)
- Remove ex-employee access quickly

2. Endpoint Protection

- Full-disk encryption
- Antivirus (CrowdStrike, SentinelOne)
- Enrol in MDM (Intune, JAMF)

3. Data Management

- Encrypt sensitive documents
- Use 1Password or Bitwarden
- Automate backups

4. Developer Hygiene

- No secrets in code
- Use env files with .gitignore
- Credential scanning: TruffleHog, GitLeaks

5. Cloud Security

- MFA everywhere
- Enable logging (CloudTrail, etc.)
- Audit IAM permissions
- Block public buckets

Monitoring & Alerting Checklist

6. Incident Response

- Document basic plan
- Shared alert channels
- Log root cause & learnings

7. Awareness & Training

- Staff training on phishing
- Internal policy handbook
- Bi-annual security reviews

Maintainer

Adesoji Adejoro

Site Reliability & Tech Support Lead

https://www.adesoji.dev